UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

TACOMA DIVISION

CHARLES METHVIN and JENNIFER CANTERBURY, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

NORTHWEST SURGICAL SPECIALISTS, P.C., A WASHINGTON PROFESSIONAL CORPORATION d/b/a REBOUND ORTHOPEDICS & NEUROSURGERY.

Defendant.

Case No. 3:25-cv-05130

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Charles Methvin and Jennifer Canterbury ("Plaintiffs"), through their attorneys, individually and on behalf of all others similarly situated, bring this Class Action Complaint against Defendant Northwest Surgical Specialists, P.C., A Washington Professional Corporation d/b/a Rebound Orthopedics & Neurosurgery ("Rebound" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiffs allege the following on information and belief—except as to their own actions, counsel's investigations, and facts of public record.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

NATURE OF ACTION

1. Defendant is a medical practice that operates 10 clinics in Washington and Oregon[1] providing orthopedic and neurosurgical care.[2] As such, Defendant stores a litany of highly sensitive personal identifiable information ("PII") and protected health information ("PHI")—together "PII/PHI"—about its current and former patients.

2. This class action arises from Defendant's *continued* failure to protect its patients' highly sensitive data.

3. In 2018 Defendant suffered a data breach that it did not reveal to patients for five months.[3]

4. But that hacking was not an isolated incident—rather, it was simply part and parcel of Defendant's pattern of negligence data security.

5. Because in 2024, Defendant experienced a *second* data breach. This class action arises from that second data breach (the "Data Breach").

6. Plaintiffs are Data Breach victims, having received a breach notice—attached as Exhibit A. They bring this class action on behalf of themselves, and all others harmed by Defendant's misconduct.

7. The exposure of one's PII/PHI to cybercriminals is a bell that cannot be unrung. Before this data breach, the private information of Defendant's patients was exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

PARTIES

8. Plaintiff, Charles Methvin, is a natural person and citizen of Washington. He resides in Kennewick, Washington where he intends to remain.

---

[1] *our locations*, REBOUND, https://www.reboundmd.com/locations (last visited Feb. 13, 2025).
[2] *about us*, REBOUND, https://www.reboundmd.com/about-us (last visited Feb. 13, 2025).
[3] Chrissy Booker, *Neurosurgery's customer systems down; health care provider won't confirm if cyberattack occurred*, THE COLUMBIAN (Feb. 7, 2024), https://www.columbian.com/news/2024/feb/07/rebound-orthopedics-health-care-provider-wont-confirm-if-data-breach-occurred/.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

9. Plaintiff Jennifer Canterbury is a natural person and citizen of Washington. She resides in Vancouver, Washington where she intends to remain.

10. Defendant, Northwest Surgical Specialists, P.C., A Washington Professional Corporation d/b/a Rebound Orthopedics & Neurosurgery, is a Washington Professional Service Corporation with its principal place of business at 200 NE Mother Joseph Place, Suite 210, Vancouver, WA 98664.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Members of the proposed Class are citizens of different states than Defendant and there are over 100 putative Class members.

12. This Court has personal jurisdiction over Defendant because it is headquartered in Washington, regularly conducts business in Washington, and has sufficient minimum contacts in Washington.

13. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

BACKGROUND

Defendant Collected and Stored the PII/PHI of Plaintiff and the Class

14. Defendant is a health care provider offers "customized treatment plans and an array of surgical, nonsurgical, and expert medical care."[4]

15. Defendant states it "proudly serve[s] the Vancouver community at our Vancouver, Salmon Creek, and Camas offices, and the Portland region at our Rose Quarter and Lake Oswego

[4] *about us*, REBOUND, https://www.reboundmd.com/about-us (last visited Feb. 13, 2025).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

offices. Through our team of sports medicine specialists, we are proud to be the team physicians for the Portland Trail Blazers, the Portland Winterhawks, and several collegiate and high school teams."[5]

16. As part of its business, Defendant receives and maintains the PII/PHI of thousands of its current and former patients.

17. In collecting and maintaining the PII/PHI, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiffs and Class members themselves took reasonable steps to secure their PII/PHI.

18. Under state and federal law, businesses like Defendant have duties to protect patients' PII/PHI and to notify them about breaches.

19. Defendant recognizes these duties. For example, in its "Notice of Privacy Practices,"[6] Defendant declares that:

a. "Proliance is committed to honoring the privacy of individuals."

b. "Proliance will not disclose any personal information obtained through the Proliance site."[7]

20. Furthermore, via its "Notice of Privacy Practices," Defendant promises its patients that:

a. "We are committed to protecting your personal medical information."

b. "The following categories describe different ways that we use and disclose PHI… YOUR WRITTEN AUTHORIZATION IS REQUIRED FOR OTHER USES AND DISCLOSURES."

---

[5] *Id.*
[6] *privacy policy,* REBOUND, https://www.reboundmd.com/about-us/privacy-policy (last visited Feb. 13, 2025).
[7] *Id.*

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

c. "Other uses and disclosures of PHI not covered by this Notice or the laws that apply to us will be made only with your written authorization."[8]

21. Defendant further declares that "[y]ou have the right to be notified in the event of a breach of your unsecured PHI."[9]

22. Elsewhere, Defendant states that it "Optimiz[es] advancement, creativity and technology to improve the quality of life for our patients, providers, and staff."[10]

Defendant's Data Breach

23. Unfortunately, Defendant's Data Breach is not an isolated incident—rather, it is simply part and parcel of Defendant's pattern of negligence data security.

24. After all, this Data Breach is the *second time* that Defendant experienced a data breach within the past several years.[11]

25. On or around February 3, 2024, Defendant was hacked.[12]

26. The hack shut down Defendant's system for several weeks, delaying one patient's ability to receive her disability payments.[13] All the while, Defendant refused to inform its patients or the public why its systems had gone down.[14]

27. Worryingly, Defendant has admitted that an "unauthorized actor accessed certain systems in the environment between February 1, 2024 and February 3, 2024 and viewed or *copied* certain files stored on these systems."[15]

28. Thus, cybercriminals copied and stole Defendant's current and former patients' highly sensitive PII/PHI, including:

a. names;

---

[8] *Id.*
[9] *Id.*
[10] *about us*, REBOUND, https://www.reboundmd.com/about-us (last visited Feb. 13, 2025).
[11] *See* n. 3.
[12] Ex. A.
[13] Chrissy Booker, *System problems continue at Rebound Orthopedics & Neurosurgery*, THE COLUMBIAN (Feb. 20, 2024), https://www.columbian.com/news/2024/feb/20/system-problems-continue-at-rebound-orthopedics-neurosurgery/.
[14] *Id.*; *see* n. 3.
[15] Ex. A (emphasis added).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

b. medical information;

c. health insurance information;

d. Social Security numbers;

e. financial account information;

f. driver license numbers;

g. passport numbers; and,

h. dates of birth.[16]

29. Stunningly, Defendant appears to have delayed notifying its current and former patients until February 4, 2025—over *one year after* the Data Breach.[17]

30. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

31. Currently, the precise number of persons injured is unclear. But upon information and belief, the size of the putative class can be ascertained from information in Defendant's custody and control. And upon information and belief, the putative class is over one hundred members—as it includes Defendant's current and former patients.

32. And when Defendant did notify Plaintiffs and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiff and the Class:

a. "Please review the instructions contained in the attached Steps You Can Take to Protect Personal Information."

b. "Rebound Orthopedics encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements and monitor free credit reports for suspicious activity and to detect errors."

[16] *Id.*
[17] *Id.*

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

c. "We also encourage you to review the enclosed Steps You Can Take to Protect Personal Information and enroll in the credit monitoring services we are offering."[18]

33. Defendant failed its duties when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII/PHI. And thus, Defendant caused widespread injury and monetary damages.

34. Since the breach, Defendant has "implemented additional safeguards to increase our security posture."[19]

35. But this is too little too late. Simply put, these measures—which Defendant now recognizes as necessary—should have been implemented *before* the Data Breach.

36. On information and belief, Defendant failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

37. Further, the Notice of Data Breach shows that Defendant cannot—or will not—determine the full scope of the Data Breach, as Defendant has been unable to determine precisely what information was stolen and when.

38. Defendant has done little to remedy its Data Breach. True, Defendant has offered some Class members basic credit monitoring. But upon information and belief, such rudimentary offerings are wholly insufficient given the scope of the Data Breach.

39. Because of Defendant's Data Breach, the sensitive PII/PHI of Plaintiffs and Class members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiffs and Class members.

40. Upon information and belief, the cybercriminals in question are particularly sophisticated. After all, the cybercriminals: (1) defeated the relevant data security systems, (2) successfully encrypted files and systems, and (3) actually *removed* sensitive files.[20]

[18] *Id.*
[19] *Id.*
[20] *See Id.*

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

41. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the dark web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[21]

42. Thus, on information and belief, Plaintiffs' and the Class's stolen PII/PHI has already been published—or will be published imminently—by cybercriminals on the dark web.

Plaintiffs' Experiences and Injuries

Plaintiff Charles Methvin

43. Plaintiff Methvin is a patient of Defendant—having received medical services from approximately 2019 to 2020.

44. Thus, Defendant obtained and maintained Plaintiff Methvin's PII/PHI.

45. As a result, Plaintiff Methvin was injured by Defendant's Data Breach.

46. As a condition of receiving medical services from Defendant, Plaintiff Methvin provided Defendant with his PII/PHI. Defendant used that PII/PHI to facilitate its provision of medical services.

47. Plaintiff Methvin provided his PII/PHI to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

48. Plaintiff Methvin reasonably understood that a portion of the funds paid to Defendant would be used to pay for adequate cybersecurity and protection of PII/PHI.

49. Plaintiff Methvin received a Notice of Data Breach dated February 4, 2025.

50. Thus, on information and belief, Plaintiff Methvin's PII/PHI has already been published—or will be published imminently—by cybercriminals on the dark web.

[21] Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

51. Through its Data Breach, Defendant compromised at least Plaintiff Methvin's:

a. name;

b. medical information;

c. health insurance information;

d. Social Security number;

e. financial account information;

f. driver license number;

g. passport number; and,

h. dates of birth.[22]

52. Plaintiff Methvin has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

53. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach.

54. Because of Defendant's Data Breach, Plaintiff Methvin has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Methvin's injuries are precisely the type of injuries that the law contemplates and addresses.

55. Plaintiff Methvin suffered actual injury from the exposure and theft of his PII/PHI—which violates his rights to privacy.

56. Plaintiff Methvin suffered actual injury in the form of damages to and diminution in the value of his PII/PHI. After all, PII/PHI is a form of intangible property—property that Defendant was required to adequately protect.

57. Plaintiff Methvin suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's PII/PHI right in the hands of criminals.

[22] *Id.*

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

58. Because of the Data Breach, Plaintiff Methvin anticipates spending considerable amounts of time and money to try and mitigate h injuries.

59. Today, Plaintiff Methvin has a continuing interest in ensuring that his PII/PHI—which, upon information and belief, remains backed uisp in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Jennifer Canterbury

60. Plaintiff Canterbury is a former patient of Defendant.

61. When Plaintiff Canterbury became a patient, Defendant required Plaintiff Canterbury provide it with substantial amounts of her PII/PHI.

62. On or about February 4, 2025, Plaintiff Canterbury received the Notice of Data Breach, which told her that her PII/PHI had been accessed during the Data Breach. Specifically, the Notice informed her that the Private Information stolen included her "name, medical information, health insurance information, Social Security numbers, financial account information, driver's license number, passport number, and date of birth."

63. The Notice also only offered Plaintiff Canterbury one year of credit monitoring services. One year of credit monitoring is not sufficient given that Plaintiff Canterbury will now experience a lifetime of increased risk of identity theft, including but not limited to, potential medical fraud.

64. Plaintiff Canterbury suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach, as well as the time she must now spend reviewing and monitoring her accounts for fraud.

65. Plaintiff Canterbury would not have provided her Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its patients' personal and health information from theft, and that those systems were subject to a data breach.

66. Plaintiff Canterbury suffered actual injury in the form of having her PII and PHI stolen as a result of the Data Breach.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

67. Plaintiff Canterbury suffered actual injury in the form of damages to and diminution in the value of her personal and health information – a form of intangible property that Plaintiff Canterbury entrusted to Defendant for the purpose of receiving healthcare services from Defendant and which was compromised in, and as a result of, the Data Breach.

68. Plaintiff Canterbury suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her PII/PHI being placed in the hands of criminals.

69. Plaintiff Canterbury has a continuing interest in ensuring that her PII/PHI, which remains in the possession of Defendant, is protected and safeguarded from future breaches. This interest is particularly acute, as Defendant's systems have already been shown to be susceptible to compromise and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its patients' PII/PHI.

70. As a result of the Data Breach, Plaintiff Canterbury made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant. Plaintiff Canterbury has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

71. As a result of the Data Breach, Plaintiff Canterbury has suffered anxiety as a result of the release of her PII/PHI, which she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her PII/PHI for purposes of committing cyber and other crimes against her including, but not limited to, fraud and identity theft. Plaintiff Canterbury is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach would have on her life.

72. Plaintiff Canterbury also suffered actual injury from having her PII/PHI compromised as a result of the Data Breach in the form of (a) damage to and diminution in the

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

value of her PII/PHI, a form of property that Defendant obtained from Plaintiff Canterbury; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

73. As a result of the Data Breach, Plaintiff Canterbury anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

74. Because of Defendant's failure to prevent the Data Breach, Plaintiffs and Class members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their PII/PHI is used;

b. diminution in value of their PII/PHI;

c. compromise and continuing publication of their PII/PHI;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII/PHI; and

h. continued risk to their PII/PHI—which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII/PHI.

75. Stolen PII/PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII/PHI can be worth up to $1,000.00 depending on the type of information obtained.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

76. The value of Plaintiffs and Class's PII/PHI on the black market is considerable. Stolen PII/PHI trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "dark web"—further exposing the information.

77. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII/PHI far and wide.

78. One way that criminals profit from stolen PII/PHI is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII/PHI, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

79. The development of "Fullz" packages means that the PII/PHI exposed in the Data Breach can easily be linked to data of Plaintiffs and the Class that is available on the internet.

80. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class members' stolen PII/PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

81. Defendant disclosed the PII/PHI of Plaintiffs and Class members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII/PHI of Plaintiffs and Class members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII/PHI.

82. Defendant's failure to promptly and properly notify Plaintiffs and Class members of the Data Breach exacerbated Plaintiffs and Class members' injury by depriving them of the

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

earliest ability to take appropriate measures to protect their PII/PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

83. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

84. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.[23] Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[24] Those 330 reported breaches exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[25]

85. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[26]

86. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[27]

87. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Failed to Follow FTC Guidelines

---

[23] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://notified.idtheftcenter.org/s/.

[24] *Id*.

[25] *Id*.

[26] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[27] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited Sept. 11, 2023).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

88. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

89. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[28] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

90. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

91. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

92. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"),

[28] *Protecting Personal Information: A Guide for Business,* FEDERAL TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

93. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to patients' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

94. Several best practices have been identified that—at a *minimum*—should be implemented by healthcare entities like Defendant. These industry standards include educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

95. Other industry standard best practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

96. The National Institute of Standards and Technology ("NIST") also recommends certain practices to safeguard systems, such as the following:

a. Control who logs on to your network and uses your computers and other devices.
b. Use security software to protect data.
c. Encrypt sensitive data, at rest and in transit.
d. Conduct regular backups of data.
e. Update security software regularly, automating those updates if possible.
f. Have formal policies for safely disposing of electronic files and old devices.
g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

97. Further still, the United States Cybersecurity and Infrastructure Security Agency

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

("CISA") makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[29]

98. Defendant failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiff's and Class Members' PII/PHI, resulting in the Data Breach.

Defendant Violated HIPAA

99. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly

[29] *Shields Up: Guidance for Organizations*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/shields-guidance-organizations (last visited Feb. 12, 2025).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[30]

100. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII/PHI and PHI is properly maintained.[31]

101. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to

[30] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[31] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

102. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

CLASS ACTION ALLEGATIONS

103. Plaintiffs bring this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII/PHI was compromised in the Data Breach discovered by Defendant in February 2024, including all those individuals who received notice of the Data Breach.

104. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

105. Plaintiffs reserve the right to amend the class definition.

106. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

107. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some individuals and sent them data breach notices.

108. Numerosity. The Class members are so numerous that joinder of all Class members is impracticable. Upon information and belief, the proposed Class includes at least one hundred members.

109. Typicality. Plaintiffs' claims are typical of Class members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

110. Adequacy. Plaintiffs will fairly and adequately protect the proposed Class's common interests. Their interests do not conflict with Class members' interests. And Plaintiffs have retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

111. Commonality and Predominance. Plaintiffs' and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class members—for which a class wide proceeding can answer for all Class members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's PII/PHI;

b. if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

c. if Defendant were negligent in maintaining, protecting, and securing PII/PHI;

d. if Defendant breached contract promises to safeguard Plaintiff and the Class's PII/PHI;

e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendant's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiff and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiffs and the Class are entitled to damages, treble damages, and or injunctive relief.

112. Superiority. A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Class)

113. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

114. Plaintiffs and the Class entrusted their PII/PHI to Defendant on the premise and with the understanding that Defendant would safeguard their PII/PHI, use their PII/PHI for business purposes only, and/or not disclose their PII/PHI to unauthorized third parties.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

115. Defendant owed a duty of care to Plaintiffs and Class members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII/PHI in a data breach. And here, that foreseeable danger came to pass.

116. Defendant has full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiffs and the Class could and would suffer if their PII/PHI was wrongfully disclosed.

117. Defendant owed these duties to Plaintiffs and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiffs and Class members' PII/PHI.

118. Defendant owed—to Plaintiffs and Class members—at least the following duties to:

a. exercise reasonable care in handling and using the PII/PHI in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiffs and Class members within a reasonable timeframe of any breach to the security of their PII/PHI.

119. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiffs and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiffs and Class members to take appropriate measures to protect their PII/PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

120. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII/PHI it was no longer required to retain under applicable regulations.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

121. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII/PHI of Plaintiffs and the Class involved an unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the criminal acts of a third party.

122. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential PII/PHI, a necessary part of obtaining services from Defendant.

123. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class members' PII/PHI.

124. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII/PHI entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs and the Class members' sensitive PII/PHI.

125. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII/PHI and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

126. Similarly, under HIPAA, Defendant had a duty to follow HIPAA standards for privacy and security practices—as to protect Plaintiffs' and Class members' PHI.

127. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect its PHI and by not complying with applicable regulations detailed *supra*. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of PHI that Defendant collected and stored and the foreseeable consequences of a data breach, including,

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

128. The risk that unauthorized persons would attempt to gain access to the PII/PHI and misuse it was foreseeable. Given that Defendant hold vast amounts of PII/PHI, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII/PHI —whether by malware or otherwise.

129. PII/PHI is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII/PHI of Plaintiffs and Class members' and the importance of exercising reasonable care in handling it.

130. Defendant improperly and inadequately safeguarded the PII/PHI of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

131. Defendant breached these duties as evidenced by the Data Breach.

132. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class members' PII/PHI by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the PII/PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

133. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII/PHI of Plaintiffs and Class members which actually and proximately caused the Data Breach and Plaintiffs and Class members' injury.

134. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs and Class members' injuries-in-fact.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

135. Defendant has admitted that the PII/PHI of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

136. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

137. And, on information and belief, Plaintiffs' PII/PHI has already been published—or will be published imminently—by cybercriminals on the dark web.

138. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and Class members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII/PHI by criminals, improper disclosure of their PII/PHI, lost benefit of their bargain, lost value of their PII/PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

139. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

140. Plaintiffs and Class members were required to provide their PII/PHI to Defendant as a condition of receiving medical services provided by Defendant. Plaintiffs and Class members provided their PII/PHI to Defendant or its third-party agents in exchange for Defendant's medical services.

141. Plaintiffs and Class members reasonably understood that a portion of the funds they paid Defendant would be used to pay for adequate cybersecurity measures.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

142. Plaintiffs and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

143. Plaintiffs and the Class members accepted Defendant's offers by disclosing their PII/PHI to Defendant or its third-party agents in exchange for medical services.

144. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII/PHI to unauthorized persons.

145. In its various policies, Defendant represented that they had a legal duty to protect Plaintiffs' and Class Member's PII/PHI.

146. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and Class members with prompt and adequate notice of all unauthorized access and/or theft of their PII/PHI.

147. After all, Plaintiffs and Class members would not have entrusted their PII/PHI to Defendant in the absence of such an agreement with Defendant.

148. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

149. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

150. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

151. Defendant materially breached the contracts it entered with Plaintiffs and Class members by:

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII/PHI that Defendant created, received, maintained, and transmitted.

152. In these and other ways, Defendant violated its duty of good faith and fair dealing.

153. Defendant's material breaches were the direct and proximate cause of Plaintiffs' and Class members' injuries (as detailed *supra*).

154. And, on information and belief, Plaintiffs' PII/PHI has already been published—or will be published imminently—by cybercriminals on the dark web.

155. Plaintiffs and Class members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

THIRD CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

156. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

157. Given the relationship between Defendant and Plaintiffs and Class members, where Defendant became guardian of Plaintiffs' and Class members' PII/PHI, Defendant became a fiduciary by its undertaking and guardianship of the PII/PHI, to act primarily for Plaintiffs and Class members, (1) for the safeguarding of Plaintiffs' and Class members' PII/PHI; (2) to timely notify Plaintiffs and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

158. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their PII/PHI.

159. Because of the highly sensitive nature of the PII/PHI, Plaintiffs and Class members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII/PHI had they known the reality of Defendant's inadequate data security practices.

160. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class members' PII/PHI.

161. Defendant also breached its fiduciary duties to Plaintiffs and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

162. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

FOURTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

163. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

164. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII/PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

165. Defendant owed a duty to its current and former patients, including Plaintiffs and the Class, to keep this information confidential.

166. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs and Class members' PII/PHI is highly offensive to a reasonable person.

167. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Class disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

168. The Data Breach constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

169. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

170. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

171. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

172. As a proximate result of Defendant's acts and omissions, the private and sensitive PII/PHI of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages (as detailed *supra*).

173. And, on information and belief, Plaintiffs' PII/PHI has already been published—or will be published imminently—by cybercriminals on the dark web.

174. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII/PHI are still maintained by Defendant with their inadequate cybersecurity system and policies.

175. Plaintiffs and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII/PHI of Plaintiffs and the Class.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

176. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other Class members, also seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

177. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

178. This claim is pleaded in the alternative to the breach of implied contract claim.

179. Plaintiffs and Class members conferred a benefit upon Defendant. After all, Defendant benefitted from using their payment and PII/PHI to provide medical services. Furthermore, Defendant benefitted from using their PII/PHI to collect payment.

180. Defendant appreciated or had knowledge of the benefits it received from Plaintiffs and Class members (or their third-party agents). And Defendant benefited from receiving Plaintiffs' and Class members' payment and PII/PHI, as they was used to provide medical services.

181. Plaintiffs and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

182. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class members' PII/PHI.

183. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class members by utilizing cheaper, ineffective security measures. Plaintiffs and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

184. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and Class members' PII/PHI and payment because Defendant failed to adequately protect their PII/PHI.

185. Plaintiffs and Class members have no adequate remedy at law.

186. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiffs and Class members—all unlawful or inequitable proceeds that it received because of its misconduct.

SIXTH CAUSE OF ACTION
Violation of the Washington Consumer Protection Act
RCW 19.86.010, *et seq*.
(On Behalf of Plaintiffs and the Class)

187. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

188. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

189. Defendant is a "person" as described in RWC 19.86.010(1).

190. Defendant engages in "trade" and "commerce" as described in RWC 19.86.010(2) in that they engage in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

191. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the CPA, in that Defendant's practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

192. Defendant's failure to safeguard the PII/PHI exposed in the Data Breach constitutes an unfair act that offends public policy.

193. Defendant's failure to safeguard the PII/PHI compromised in the Data Breach caused substantial injury to Plaintiffs and Class Members. Defendant's failure is not outweighed

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

by any countervailing benefits to consumers or competitors, and it was not reasonably avoidable by consumers.

194. Defendant's failure to safeguard the PII/PHI disclosed in the Data Breach, and its failure to provide timely and complete notice of that Data Breach to the victims, is unfair because these acts and practices are immoral, unethical, oppressive, and/or unscrupulous.

195. In the course of conducting their business, Defendant committed "unfair or deceptive acts or practices" by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and Class Members' PII/PHI, and violating the common law alleged herein in the process. Plaintiffs and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. As described above, Defendant's wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

196. Defendant also violated the CPA by failing to timely notify, and by concealing from Plaintiffs and Class Members, information regarding the unauthorized release and disclosure of their PII/PHI. If Plaintiffs and Class Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their PII/PHI and identities.

197. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair or deceptive acts or practices" in violation of the CPA in that Defendant's wrongful conduct is substantially injurious to other persons, had the capacity to injure other persons, and has the capacity to injure other persons.

198. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

199. Defendant's unfair or deceptive acts or practices occurred in its trade or business and have and injured and are capable of injuring a substantial portion of the public. Defendant's general course of conduct as alleged herein is injurious to the public interest, and the acts complained of herein are ongoing and/or have a substantial likelihood of being repeated.

200. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violations of the CPA, Plaintiffs and Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*, (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of their PII/PHI; (5) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (6) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

201. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiffs, therefore, on behalf of themselves and the Class, seek restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII/PHI entrusted to it.

202. Plaintiffs, on behalf of themselves and Class Members, also seek to recover actual damages sustained by each Class Member together with the costs of the suit, including reasonable attorney fees. In addition, Plaintiffs, on behalf of themselves and Class Members, request that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each Class Member by three times the actual damages sustained not to exceed $25,000.00 per Class Member.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

SEVENTH CAUSE OF ACTION
Violation of the Washington Data Breach Disclosure Law
RCW 19.255.005, *et seq*.
(On Behalf of Plaintiffs and the Class)

203. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

204. Under RCW § 19.255.010(2), "[a]ny person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

205. Upon information and belief, this statute applies to Defendant because Defendant does not own nor license the PII/PHI in question. Instead, the owners and/or licensees of the PII/PHI are Plaintiffs and the Class.

206. Here, the Data Breach led to "unauthorized acquisition of computerized data that compromise[d] the security, confidentiality, [and] integrity of personal information maintained by" Defendant, leading to a "breach of the security of [Defendant's] systems," as defined by RCW § 19.255.010.

207. Defendant failed to disclose that the PII/PHI—of Plaintiffs and Class Members—that had been compromised "immediately" upon discovery, and thus unreasonably delayed informing Plaintiffs and the proposed Class about the Data Breach.

208. In fact, Defendant appears to have delayed notifying its current and former patients until November 21, 2023—a full two-hundred and eighty-three (283) days *after* the Data Breach.

209. Thus, Defendant violated the Washington Data Breach Disclosure Law.

EIGHTH CAUSE OF ACTION
Violation of the Washington Uniform Health Care Information Act (UHCIA)
RCW 70.02.005, *et seq*.
(On Behalf of Plaintiffs and the Class)

210. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

211. UHCIA declares that:

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

a. "Health care information is personal and sensitive information that if improperly used or released may do significant harm to a patient's interests in privacy, health care, or other interests." § 70.02.005(1).

b. "In order to retain the full trust and confidence of patients, health care providers have an interest in assuring that health care information is not improperly disclosed and in having clear and certain rules for the disclosure of health care information." § 70.02.005(3).

c. "It is the public policy of this state that a patient's interest in the proper use and disclosure of the patient's health care information survives even when the information is held by persons other than health care providers." § 70.02.005(4).

212. Here, Defendant is a "health care provider" because Defendant "is licensed, certified, registered, or otherwise authorized by the law of this state to provide health care in the ordinary course of business or practice of a profession." § 70.02.010(19).

213. Under § 70.02.020, "a health care provider, an individual who assists a health care provider in the delivery of health care, or an agent and employee of a health care provider may not disclose health care information about a patient to any other person without the patient's written authorization."

214. Here, Defendant violated UHCIA because Defendant—via its Data Breach—disclosed health care information to third parties without patient authorization.

NINTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiffs and the Class)

215. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

216. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

217. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiffs alleges that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiffs and Class members continue to suffer injury from the ongoing threat of fraud and identity theft.

218. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiffs and Class members.

219. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

220. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

221. And if a second breach occurs, Plaintiffs and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiff and Class members' injuries.

222. If an injunction is not issued, the resulting hardship to Plaintiffs and Class members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

223. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiffs, Class members, and the public at large.

PRAYER FOR RELIEF

Plaintiffs and Class members respectfully request judgment against Defendant and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiffs and the Class;

D. Awarding Plaintiffs and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

E. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

F. Awarding attorneys' fees and costs, as allowed by law;

G. Awarding prejudgment and post-judgment interest, as provided by law;

H. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial for all claims so triable.

Dated: February 17, 2025

By: */s/ Samuel J. Strauss*
Samuel J. Strauss, WSBA #46971
Raina C. Borrelli*
STRAUSS BORRELLI PLLC
980 N Michigan Ave, Suite 1610

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

Chicago, IL 60611
(872) 263-1100
sam@straussborrelli.com
raina@straussborrelli.com

Tyler J. Bean*
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: tbean@sirillp.com

**Pro Hac Vice Forthcoming*

Attorneys for Plaintiffs and the Proposed Class